(54) **MUTUAL AUTHENTICATION SYSTEM FOR INFORMATION RECORDING MEDIUM**

(57) Abstract:

PROBLEM TO BE SOLVED: To make a system excellent in security by storing master keys and algorithms needed in operations of mutual authentications by terminals in security modules in readout impossible states to make the keys and the algorithms not to be stolen.

SOLUTION: Same terminal main bodies can be used as terminal main bodies 1 even for systems whose users are different. In security modules 2 to be used in a system A, modules in which master keys As and functions (fs) are used are used and in security modules 2a to be used in a system B, modules in which master keys Bs and functions (gs) are used are used for the common main bodies 1. Then, respective terminals 10, 10b for system A, system B can be constituted by building up security modules different in respective systems in common terminal main bodies. Thus, master keys and algorithms are never abused by being decoded illegally from the outside and the high security of this sysyem is kept.